学術情報基盤オープンフォーラム
「大学のクラウド活用における、検証と課題と対策」

クラウド時代に気をつけたいセキュリティ

セキュリティe-learningコンテンツと学認について

岡部 寿男（京都大学）

国立情報学研究所 学術情報ネットワーク運営・連携本部
- 認証作業部会 学認タスクフォース
- 高等教育機関におけるセキュリティポリシー推進部会

クラウドのセキュリティと学認

- クラウドの本質はアウトソーシング
  - サービスを外へ出し分散しつつセキュリティとプライバシーを守るためには、認証と認可の一元化が必須

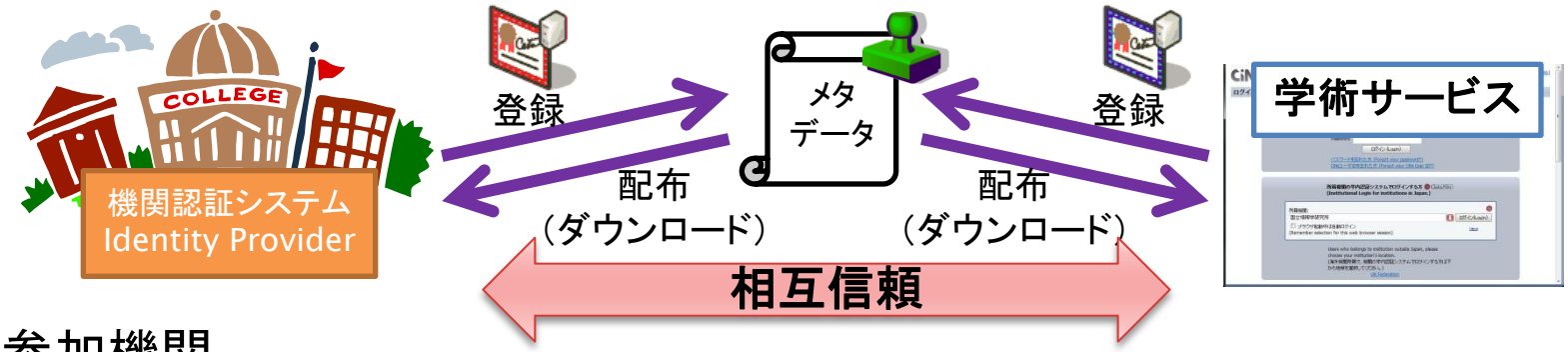
  ⇒機関をまたがる認証連携が鍵：学認
    - 保証のレベル LoA (Level of Assurance)の認定
    - 民間サービスとの高度な連携の可能性：SITF
- クラウドのキーワードはスケールメリット
  - サービスの単純化、共通化、集約により、品質向上とコストダウンを同時に達成

  ⇒SaaSとしての、学認連携情報セキュリティe-learning

学認による認証連携の基礎

GakuNin ポリシーに準拠し参加機関間の認証連携を実現

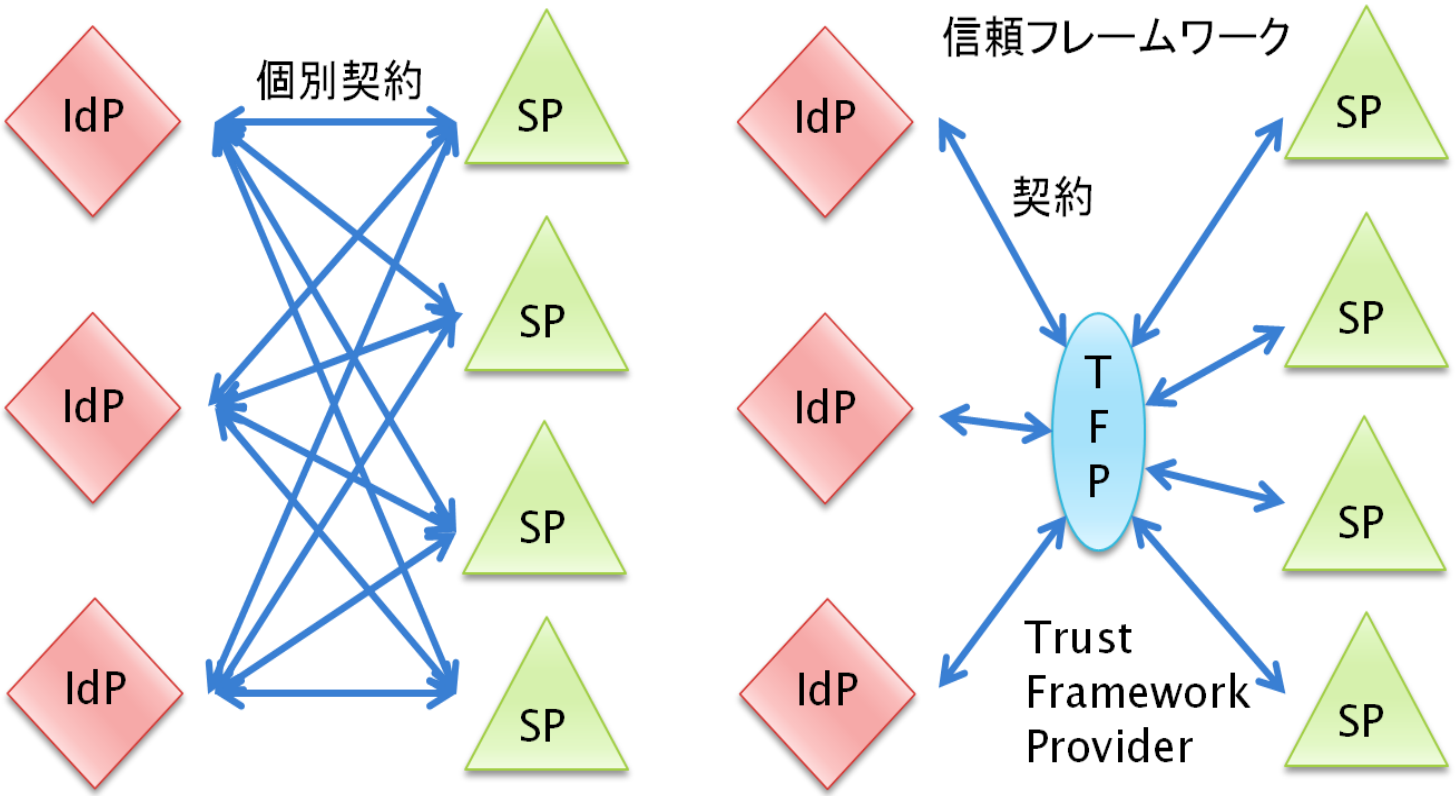
- 学術認証フェデレーション実施要領(平成24年3月22日 改正)
- 学術認証フェデレーション システム運用基準 (Ver.1.2)(平成23年8月24日 改正)



- 参加機関
  - ポリシーに準拠することにより学認に参加可能
- 事務局
  - 参加が承認されたIdPとSPの情報はメタデータに登録
- IdP,SPサーバ
  - メタデータに登録されたIdPとSPだけが互いに接続することができる

信頼フレームワークの効果

- 一律のポリシー、インタフェース基準に基づく信頼フレームワークの導入により、個別契約でのN×Mの関係が、N＋Mの関係に縮減



学認における信頼の構築

- 学認で定める技術仕様と運用ルール
  - 学術認証フェデレーション実施要領
  - 学術認証フェデレーション システム運用基準
    - 一律の規定（ポリシー）を信頼し合うことで、IdPとSPの間で相互接続が可能に
    - 信頼関係（トラストサークル）を保つことは、参加機関に対して「学認」が果たすべき重要な役割
- 定期的な確認
  - 各機関にIdP運用の自己評価アンケートを実施（年１回）
  - アンケートの内容は，ポリシーに基づいた運用を確認する簡単なもの

システム運用基準で定めるIdPの要件

- 組織の構成員であることの保証
  - 卒業、退職などによる異動の適切な反映
  - 名誉教授、OB、図書館の地域内利用者、その他ゲスト等の扱い
- 識別子再利用についての考慮
  - 同一識別子を利用する場合は、一定期間あける
- ユーザの同一性の保証
  - パスワード配布時の本人確認
  - 適切に管理された役職アカウント
- 個人情報保護への対応
  - 国公立大学ではオプトインが原則
- ログの保存
  - インシデント対応のための、eduPersonTargetdIDやtransient-idの記録

機関として責任を持った
IDおよび属性の保証

⇒定期アンケート（毎年）によるチェックとフィードバックで維持

Level of Assurance

- NIHのサービスを学認SPとして利用
  - 米国連邦政府内のサービス(SP)を、外部の認証システム(IdP)に接続する場合には、SP側がIdPの保証レベル(Level of Assurance, LoA)を要求。
  - 4つのレベルを規定
    - レベル1:whitehouse.govのWebサイトでのオンラインディスカッションに参加
    - レベル2:社会保障Webサイトを通じて自身の住所記録を変更
    - レベル3:特許弁理士が特許商標局に対し、機密の特許情報を電子的に提出
    - レベル4:法執行官が、犯罪歴が格納されている法執行データベースにアクセス
  - PubMedの要求はLevel 1(最低)であり、利用するためには学認のIdPが米国の基準に則ったLevel 1を取得する必要あり。

2012年7月、学認においてOIX LoA1認定プログラムを開始

NISTのLoA 技術要件(NIST SP 800-63)

- **レベル1**　翻訳版：http://www.ipa.go.jp/security/publications/nist/documents/SP800-63-J.pdf
  - ユーザの同一性を保証（身元識別は不要）、認証の有効期限なし
  - チャレンジ-レスポンス可（辞書攻撃に弱い）
- **レベル2**　*（実際には学認はおおよそこのレベル）*
  - 単一要素認証、身元識別あり、失効処理の保証
  - オンライン推測攻撃を防止すること（パスワード/TLS可）
  - 認証サーバでの平文パスワード保持の禁止
- **レベル3**
  - **多要素認証**、ソフト暗号化トークン使用可
  - なりすまし攻撃、中間者攻撃を防止すること
- **レベル4**
  - 実用上最大限の保証、ハード暗号化トークンを使用
  - 認証後の暗号化処理も認証プロセスに結びつく鍵を使用

ISO/IEC 29115 (Entity Authentication Assurance Framework)として標準化作業中

学認としての新たな展開の可能性

- e-Radの次期システムがSAMLに対応
- e-RadとReaD&ResarchMapの連携
  - 業績データの連携操作を、SAMLによるSSOで実現

学認との親和性が向上

- 米国ではNSFグラント申請システムと学術認証フェデレーションInCommonを、Level2を条件に接続

学認としてLevel 2のTFP獲得を目指す
https://www.gakunin.jp/docs/fed/loa

さらなる拡大に向けて：OpenIDとの連携

- 民間デファクトであるOpenID対応のサービスが、学認IdPで認証して利用できるようになれば、**学認（大学）向けのサービス**がさらに広がる
  - 学認にて**プロトコルゲートウェイ**によるOpenID Connect対応

- 民間（OpenID OP）から 学認対応SP へのアクセスが可能になれば、**産学協同研究の情報基盤**としての活用や**保護者向けサービス**へも展開できる
  - Google/Yahooなどのアカデミックサービスを利用している大学の、学認参加も容易に

学認で扱う属性情報（IdPからSPへ送出）

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の匿名識別子
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種（@scopeつき）
eduPersonEntitlement	資格
SurName (sn)	氏名（姓）
jaSurName (jasn)	氏名（姓）（日本語）
GivenName	氏名（名）
jaGivenName	氏名（名）（日本語）
displayName	氏名（表示名）
jaDisplayName	氏名（表示名）（日本語）
mail	メールアドレス
gakuninScopedPersonalUniqueCode	学生・職員番号（@scopeつき）

実際に使われる属性情報の例

サービスA (1項目必須)

eduPersonPrincipalName(必須)

サービスB (1項目必須)

eduPersonAffiliation (必須)
eduPersonTargetedID

サービスC (必須項目なし)

eduPersonEntitlement
eduPersonAffiliation

必要最低限のみを送出

(参考) https://www.gakunin.jp/docs/fed/technical/attribute

SITF (Student ID Trust Framework)
「学生である」という属性情報の活用

- 学生証を提示するという行為をネットの世界でも可能に
- その属性の信頼性は？
  - 各大学が所属している学生に対して、大学の署名付きの属性を提供する
  - 一定レベルの管理がなされているかどうかを、学認がチェックし、保証する
  - よって、学認がTrust Framework Providerとして、「学生である」という属性の取り扱いに関する一定のルールを設ける
  - 属性情報に関するプライバシー保護についても考慮

⇒民間企業と学術機関・大学とのコラボレーションによって多様なサービスやイノベーションが生まれることを期待

SITFで定めるべきポリシーの検討

- LoAA: Level of Student Assurance for Attribute Provider
  - 属性プロバイダとしての大学の要件
    - 「学生」の定義の明示（大学ごとの揺れを許容）
    - 大学の努力義務と免責

- LoP: Level of Protection for Relying Party
  - 属性を利用するRPにおけるプライバシー保護に関する責務
    - 学生および大学に不利益が生じないように、取得する属性の内容とその用途を明確にし、同意を得る
    - 属性の第三者への譲渡禁止、有効期限の遵守

  など

情報セキュリティ等のe-learning

- **大学等における情報セキュリティ講習**
  - 情報セキュリティポリシーの策定に伴う要件
    - 全構成員への周知が求められる
  - オンライン化が望まれるが、大学が個別にシステムおよびコンテンツを整備するのは非効率的
- **学認と連動したサービスとして構築**
  - 受講履歴を大学にフィードバック
    - 匿名ID (ePTID) による管理
  - 初期コンテンツとして、群馬大で開発された「倫倫姫」を採用
    - 4カ国語（日、英、中、韓）対応
    - サンプル規程準拠
  - 大学オリジナルコンテンツ追加可能
- **2012年度より試行提供開始**
  - 将来的にはNIIの研修事業へ

学認連携情報セキュリティe-learning

- 共用Eラーニング SP「学認連携 Moodle 講習サイトβ」
  - 「ヒカリ＆つばさ」
    - 教職員向けコンテンツも追加準備中
  - 「倫倫姫」（群馬大学）
    - サンプル規程準拠

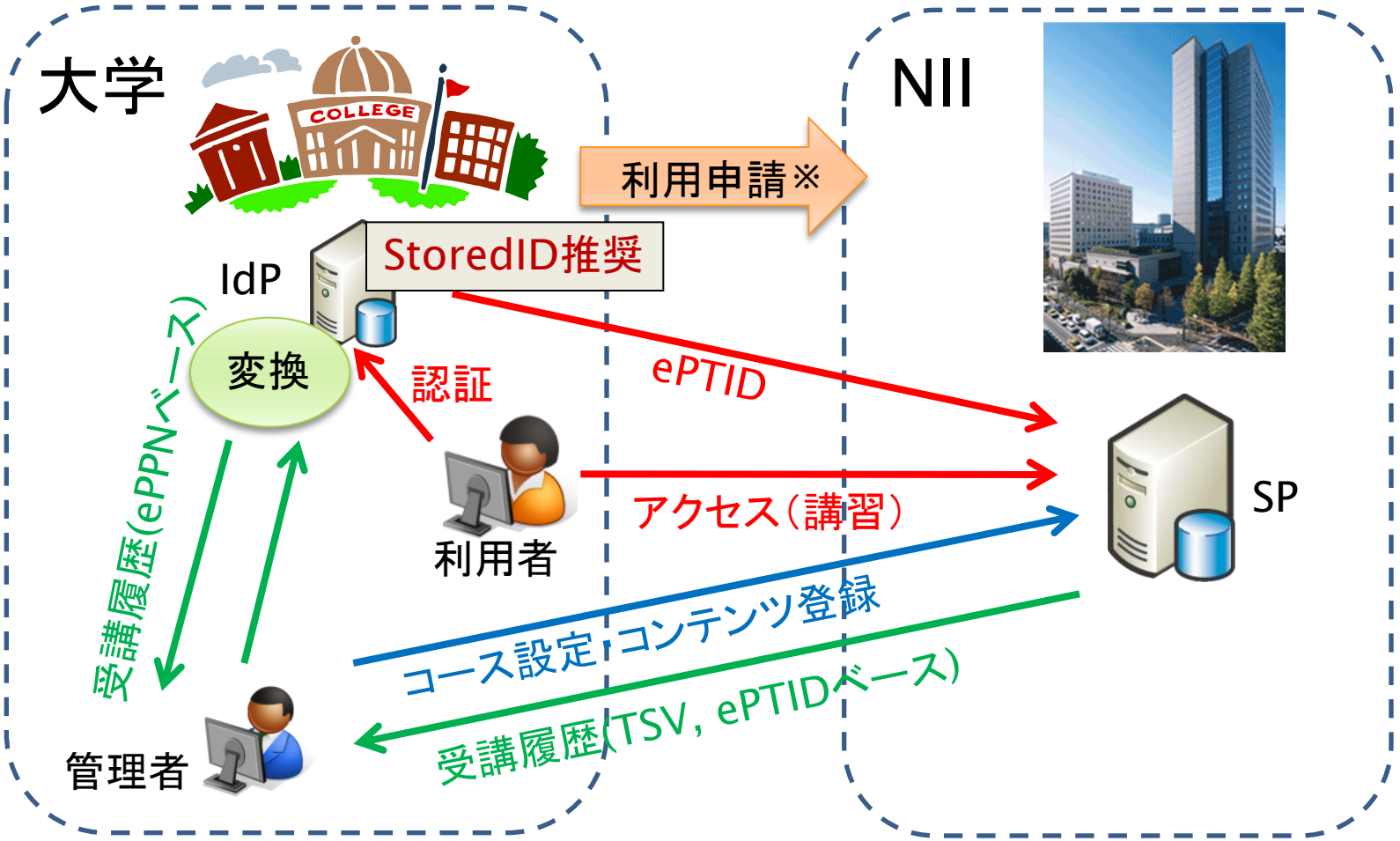
教職員・学生が受講

セキュリティラーニングシステム

受講状況を機関にフィードバック

類似サービスを各機関で個別に導入する必要なし

学認連携 Moodle 講習サイトβのしくみ



※大学からの「利用申請」がなくても自習可能

まとめにかえて

- クラウド対応認証連携としての学認
  - 国際標準に準拠したLoA (Level of Assurance)の認定
  - 民間サービスとの連携を可能にするSITF (Student ID Trust Framework)
- クラウド時代の情報セキュリティe-learning
  - セキュリティポリシーそのものの標準化・共通化
    - サンプル規程のとりくみ
  - コンテンツの共同作成・共有
    - 「ヒカリ＆つばさ」「倫倫姫」
  - SaaSとしてのe-learningの提供

【宣伝】Japan Identity & Cloud Summit
2013年3月4-5日@学術総合センター https://jics.nii.ac.jp/